MOTION PICTURE ASSOCIATION
OF AMERICA, INC.
1600 EYE STREET, NORTHWEST
WASHINGTON, D.C. 20006
(202) 293-1966
(202) 293-7674 FAX
dowt@mpaa.org

TROY DOW
VICE PRESIDENT & COUNSEL
TECHNOLOGY & NEW MEDIA

January 14, 2003

United States Patent and Trademark Office
Office of Legislative and International Affairs
2121 Crystal Drive
Arlington, VA 22202

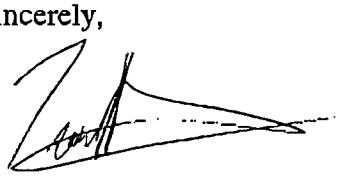
Attention: Ms. Velica Steadman

Dear Ms. Steadman:

I am pleased to submit the attached comments on behalf of the Motion Picture Association of America (MPAA) in response to the Request for Written Comments and Notice of Hearings on Technological Protection Systems for Digitized Copyrighted Works (Docket No. 2003-C-006). As indicated in the attached, MPAA will be pleased to provide to the Patent and Trademark Office whatever additional information or assistance may prove useful, including by being available to participate in the tentatively scheduled February 4 hearing.

Should you have any questions, please do not hesitate to contact me.

Sincerely,



COMMENTS OF THE MOTION PICTURE ASSOCIATION OF AMERICA: TECHNOLOGICAL PROTECTION SYSTEMS FOR DIGITIZED COPYRIGHTED WORKS

SUBMITTED TO THE U.S. PATENT AND TRADEMARK OFFICE
JANUARY 14, 2003

The Motion Picture Association of America (MPAA) is pleased to provide comments in response to the Request for Written Comments and Notice of Hearings on Technological Protection Systems for Digitized Copyrighted Works (Docket No. 2003-C-006). MPAA represents the major producers and distributors of theatrical motion pictures, home video material and television programs. MPAA members include: Buena Vista Pictures Distribution, Inc. (Disney); Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation; Sony Pictures Entertainment, Inc.; Twentieth Century Fox Film Corporation; Universal Studios, Inc.; and Warner Bros.

I. Introduction

The Request for Written Comments solicits information "on technological protection systems that have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including upgradeable and self-repairing systems, and systems that have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad based consensus process."

MPAA and its member companies place tremendous emphasis on technological protection systems, both as a means of enabling new choices and new products for consumers, and as a means of protecting capital investment in high-quality, high-value digital entertainment products. Indeed, MPAA and its member companies have all devoted substantial time, effort and resources to the development of a meaningful architecture for content protection in the digital environment, including through direct engagement with technology providers, through participation in voluntary multi-industry negotiations, and through participation in open technical standards setting processes. As a result, there is today a robust and growing market for content protection systems, and a number of technologies have been developed and implemented, or are available for implementation (noting that patent and licensing issues may remain as barriers to implementation in some cases). While progress has been made in this area, much more remains to be done, particularly given the challenges posed by the growth of virtually unchecked and wholly unauthorized viral distribution of copyrighted works via digital networks.

There is no one solution to the challenge of digital piracy. In these comments we will endeavor to describe the goals that we believe must be accomplished as part of any meaningful attempt to construct an overall framework for the protection of digitized copyrighted works and to provide examples of the types of work that is ongoing in these areas to develop technologies that fit in to such a framework. These comments are not meant in any way to provide an exhaustive list of

technologies, to be an endorsement of any particular technology, or to suggest a view as to whether or not the use of a particular technology would be sufficient for purposes of qualifying to take advantage of the limitations on exclusive rights contained in the Technology, Education and Copyright Harmonization (TEACH) Act or any other provision of the Copyright Act. They are meant merely to assist the Patent and Trademark Office and the Copyright Office in understanding the types of technologies that have been developed, are being developed, or might be developed to protect digitized copyrighted works and prevent infringement.

II. Content Protection Objectives

MPAA has described three primary goals whose attainment is necessary in order to confront the growing contagion of digital piracy and to facilitate the viability of a legitimate marketplace for high-quality digital entertainment. These are:

> Goal One: Implementing a "Broadcast Flag" to prevent the unauthorized redistribution of "in-the-clear" digital over-the-air broadcast television, including its unauthorized redistribution over the Internet.
>
> Goal Two: Plugging the "analog hole" that results from the fact that protected digital content can easily be converted into analog form and then reconverted to unprotected digital form, making it subject to widespread unauthorized copying and redistribution.
>
> Goal Three: Putting an end to the avalanche of copyright theft on so-called "file-sharing" services on peer-to-peer (p2p) networks.

The technological means of attaining each of these goals may – and often will – differ, and each will be discussed separately below. Their treatment here is not a listing in order of priority, but rather reflects the current status in terms of progress toward the realization of these goals. The attainment of each of these goals is needed in order to construct an overall framework for content protection in the digital environment.

A. Protecting digital over-the-air broadcast content (the "Broadcast Flag")

With the transition from analog to digital broadcast television comes the challenge of how to protect this high-quality digital signal from unauthorized redistribution. Protecting over-the-air digital broadcast television is a unique challenge because, unlike other digital programming distribution methods such as cable, satellite, or DVDs, digital broadcast television is transmitted "in the clear" (i.e., in unencrypted form without conditions on access), and thus is subject to an extraordinarily high risk of unauthorized redistribution. Once received in the home, digital broadcast television content can easily be redistributed via retransmission over networks like the Internet by such means as rebroadcasting, hosting files on a web server, or peer-to-peer file trafficking. Such unauthorized redistribution can be accomplished without downloading any special software, without the need for circumventing any copy protections, without such tools as analog-to-digital converters, or indeed without any complex technical skills whatsoever. Thus, without some technical means of controlling unauthorized redistribution, copyright owners are

faced with the spectre of digital piracy on a massive scale of whatever content they make available for digital broadcast.

A technical solution has been developed to meet this challenge and is available for implementation. The Advanced Television Systems Committee (ATSC) – the standards setting body responsible for voluntary technical standards for high definition television – has developed and adopted a specification for an ATSC Redistribution Control Descriptor (or "Broadcast Flag"), which is set forth in ATSC Standard A/65A: Program and System Information Protocol for Terrestrial Broadcast and Cable, 31 May 2000, Amendment 3, 6 February 2002. In very general terms, digital broadcast television content may be embedded with the Broadcast Flag to assert redistribution control, and consumer products receiving such content can identify it as flagged for protection against unauthorized redistribution and, in response, handle such content in a secure manner, including by passing such content on only to other products that will also handle it securely.

In November 2001, the inter-industry Copy Protection Technical Working Group (http://www.cptwg.org) – made up of motion picture studios, consumer electronics manufacturers, computer and information technology manufacturers, and others – formed the Broadcast Protection Discussion Group (BPDG) to address the issue of protecting digital broadcast television signals against unauthorized redistribution and the technical sufficiency of the Broadcast Flag for this purpose. More than 70 representatives of the motion picture, consumer electronics, computer and information technology, cable and broadcast industries, as well individuals and representatives of consumer and civil liberties groups, participated in that process. On June 3, 2002, the BPDG Co-Chairs issued a "Final Report" announcing a broad inter-industry consensus on the use of the Broadcast Flag technology for digital broadcast television redistribution control and on the outlines of a Broadcast Flag "Solution". It should be noted that the Broadcast Flag Solution is not a means of "copy protection." It is a technical means of preventing unauthorized redistribution of digital broadcast television content outside the personal digital network environment. As such, the Broadcast Flag Solution does not prevent or limit the number of physical copies being made within the home. It requires only that such copies be sufficiently secure so as to prevent such copies from being a source of unauthorized redistribution outside the home.

To be effective, a Broadcast Flag Solution will require a regulatory component to ensure that consumer products containing demodulators – devices that convert the digital broadcast television signal from a radio waveform to a digital data stream – do, in fact, check for the Flag and treat flagged content securely, or treat the content as if it were flagged until it is screened for the Flag. Regulation of consumer products with modulators will also be necessary in order to prevent content that originated in another protected distribution channel, such as encrypted pay-per-view transmissions, from being mislabeled as copyable digital broadcast content and then redistributed using compliant products. The Federal Communications Commission (FCC) has issued a Notice of Proposed Rulemaking (MB Docket No. 02-230) in which it has solicited comments on the need for such a regulatory regime within the limited sphere of digital broadcast television and on whether the FCC should adopt rules or create some other mechanism to resolve any outstanding compliance, robustness and enforcement issues related to the Broadcast Flag

Solution. MPAA believes such a regime is needed and is participating actively in the FCC proceeding. A copy of the White Paper entitled "A Proposal for Protection of Unencrypted Digital Broadcast Television," which accompanied the joint filing by MPAA and 18 other organizations in the initial comment round in that proceeding, describes the Broadcast Flag Solution in greater detail and is attached to these comments.

B. Plugging the Analog Hole (Preventing Analog Reconversion)

The "Analog Hole" is a term used to describe a gap in protection that exists in digital content protection systems by virtue of the fact that digital content protection systems can generally protect content against unauthorized reproduction and distribution only in a digital environment. If protected digital content is converted to analog format (e.g., for viewing on an analog television or computer monitor), these content protection mechanisms are eliminated or reduced. This presents a problem in that digital devices can capture and digitize unprotected analog signals (including formerly protected digital signals that are stripped of their protection as they pass through analog outputs) with complete disregard for current copy protection mechanisms, thus enabling a major source of unauthorized duplication and/or redistribution. Such analog to digital conversions are easy to accomplish with the use of widely available, inexpensive PC technology and other digital recording devices with analog inputs.

The primary means to address the analog hole is via embedded watermarks (which have additional applications as will be discussed below). Watermarking is a type of copy control information (CCI) marking system. These systems allow usage rules to be conveyed with the content. Watermarking technology in particular allows for copy control information to be invisibly and securely embedded in the content, as well as markings to be embedded for forensic tracking purposes. Such watermarks are persistent and robust in that they survive the digital-to-analog conversion process and they are not easily removed. In order to help plug the analog hole, watermark detectors would be needed in all devices that perform analog to digital conversions. In such devices (e.g., PC video capture cards), the role of the watermark detector would be to detect the watermark and ensure that the device responds appropriately. The watermark would instruct the conversion device never to allow copying, allow only one copy, allow first generation copying but not serial copying, or to allow unlimited copying. MPAA has proposed an Extended Copy Control Information (ExCCI) packet for use in both analog and digital video signals that would allow even more flexibility in the content usage information that could be conveyed via watermarking and other CCI marking systems (*see* http://www.cptwg.org/Assets/September%20presentations/16).

Another form of analog CCI marking system is the Analog Copy Generation Management System (CGMS-A). CGMS-A is a technology standard that allows a set of pulses to be applied to lines in the vertical blanking interval of an analog video signal to convey copy control information. Thus, CGMS-A technology allows such information to be conveyed with the content, but unlike watermark technology, does not allow for such information to be securely embedded within the content itself.

There are a number of companies and consortia developing and offering persistent watermark technologies. These include IBM, Toshiba, Verance, the VWM Group (which includes the former Galaxy companies – Hitachi, NEC, Pioneer, and Sony – and the former Millennium companies – Digimarc, Macrovision and Philips), and undoubtedly many others.

The realization of watermarking as a vehicle in plugging the analog hole has two steps:

1. A robust watermarking technology must be selected, and

2. Compliance and enforcement rules for detection and response to this technology in various platforms (including PC and PC-like devices) must be drafted and agreed upon.

In the case of DVDs, the selection of a watermark technology has been underway since early 2001 under the auspices of the DVD Copy Control Association (DVD-CCA). Once chosen, the watermark would be implemented in conjunction with CSS licensed DVD players (both consumer electronics devices and DVD PC drives) to prevent unauthorized recording and playback of DVD content where the CSS encryption has been bypassed. While there had reportedly been considerable agreement within the DVD-CCA on a watermark technology for copy and playback control in DVD players and drives, the DVD-CCA Board was unable to reach an agreement on the selection of a technology before the dissolution of the then-current Board in August 2002. The watermark selection process is being considered by the new DVD-CCA Board, which may or may not result in a selection.

If a consensus watermark can be selected by the DVD-CCA that is agreeable to the copyright, IT and CE industries, it will only represent a solution that is specific to CSS-licensed DVD players. Comprehensively addressing such issues as the analog hole beyond DVD players will require cross-industry agreement in a cross-industry forum on how and under what compliance framework watermark or other CCI marking detection and response would take place in analog-to-digital converters. The CPTWG has recently announced the formation of a new subgroup – the Analog Reconversion Discussion Group – to discuss technologies and systems to address the analog hole problem.

C. Stopping Unauthorized Distribution on Peer-to-Peer Networks

Stemming the avalanche of unauthorized content on peer-to-peer networks is a complex problem that will require a multifaceted solution. Peer-to-peer piracy is such a difficult challenge and such a major threat to copyright owners because it combines the ease of reproduction and distribution brought about by digital technology with the amplification effect created by a viral distribution architecture in which every unauthorized copy made is in turn made available to millions for unauthorized download, such that a single copy made available for unauthorized download becomes two copies, and in turn four copies, and in turn eight, and exponentially on until the network is flooded with unauthorized perfect reproductions available for millions to download at the click of a button.

Solving this problem will require both technical means of preventing unauthorized copies of creative media from leaking out of the protected digital environment and on to p2p networks, and the means – both technical and legal – of limiting the proliferation of and access to those unauthorized copies that do escape the framework of technological protection systems.

1. Keeping Digital Content within a Protected Environment

Much work is being done to develop technological systems and architectures intended to create a secure environment for the distribution of digital content and to limit the sources of unauthorized content on p2p networks. The Broadcast Flag Solution described above is one technology aimed at preventing unencrypted over-the-air digital broadcast television from becoming a source of pirated television programming on p2p networks. Similarly, preventing analog reconversion (i.e., plugging the analog hole) through the use of watermark or other CCI marking system technology is another important effort aimed at ensuring that consumer devices with unprotected analog outputs do not continue as a long-term source of pirated content on p2p networks. A host of other technologies are available or under development – including encryption, authentication, conditional access, link protection, digital watermarking/CCI marking, and digital rights management technologies – that are intended to fit together in an overall framework that allows for the secure delivery of digital content to the home and persistent protection against unauthorized access and redistribution once the content is delivered.

One such model is the model of a "link-protected" architecture in which encryption, authentication and watermarking technologies are combined with licensing agreements to create a framework in which content is encrypted and transmitted digitally only via protected outputs and only to devices that are bound to provide a minimum level of persistent protection and, in some cases, to respond to usage rules conveyed by associated watermarks (*see* http://www.4centity.com/data/tech/cpsa/cpsa081.pdf for a description by the 4C entity of its Content Protection System Architecture (CPSA)). Such an architecture could be employed to limit content to display only, to allow the content to move freely within the personal digital network environment, or something in-between. Some of the technologies that fit within such a model include:

Content Scramble System (CSS) – The access control and copy prevention system licensed by the DVD-Copy Control Association (DVD-CCA) for use on DVDs. Digital audiovisual content on DVD is encrypted using CSS and may be decrypted only by players licensed by DVD-CCA. Licensed players must, among other things, protect against copying, protect against disclosure of the decryption keys, and not pass the content over unprotected digital outputs.

Digital Transmission Content Protection (DTCP or "5C") – Technology developed and licensed by the 5C companies – Intel, Hitachi, Matsushita, Sony and Toshiba – to provide for secure, encrypted transmission of digital content over IEEE 1394 "Firewire" and USB digital buses. Such technology might be used to protect content from unauthorized access as it is transmitted from a DVD player or other source device through a digital "Firewire" connection to a high-definition digital television set, or to ensure that DVD content is sent

via digital outputs only to devices that will recognize and follow any associated copy control instructions. *See* http://www.dtcp.com/data/wp_spec.pdf.

High-bandwidth Digital Content Protection (HDCP) – Technology developed by Intel to protect uncompressed digital content as it travels over Digital Visual Interface (DVI) links to computer monitor or television displays. *See* http://www.digital-cp.com/.

Content Protection for Recordable Media (CPRM) – Technology developed by the 4C companies – IBM, Intel, Matsushita and Toshiba – to provide protection in recordable digital media (e.g., Secure Digital Memory Cards, Secure CompactFlash, DVD video recorders). The technology provides for encryption of "copy once" content and includes the obligation to recognize and respond to watermarks and copy control instructions in content entering unprotected inputs. *See* http://www.4centity.com/tech/cprm/.

Content Protection for Prerecorded Media (CPPM) – Also developed by the 4C companies to provide protection – using encryption and watermark detection – in pre-recorded digital media. Adopted for use with the DVD Audio format. *See* http://www.4centity.com/tech/cprm/.

SmartRight – Technology developed by Thompson for use in the home network environment. Uses smart cards in devices within the home network to authenticate devices and encrypt protected content. *See* http://www.smartright.org/.

xCP Cluster Protocol – Technology developed by IBM using broadcast encryption to limit access to content to a defined "cluster" of devices within the personal digital network environment. *See* http://www.cptwg.org/Assets/Presentations/CPTWG%20-%20xCP-07-02.ppt.

Open Conditional Content Access Management (OCCAM) – An encryption based open technology standard developed by Cisco for use in protecting digital content on public, private and home networks. *See* http://www.senate.gov/~commerce/hearings/022802bechtolsheim.pdf.

Existing closed network technologies, including virtual private networks, closed cable and satellite systems, etc., may also provide protection by limiting access to content to authorized users and by ensuring appropriate downstream protection through both technology and licensing agreements similar to those described above. For example, a digital cable or satellite system can condition access to certain high-value digital content on subscriber agreements and use set-top-box embedded security or smart card technologies that treat such content in a secure manner and prevent retransmissions of such content over unprotected digital outputs.

Similarly, other software-based digital rights management (DRM) technologies have been and are being developed to provide for secure delivery of content over the Internet and adherence to copy control instructions and usage rules in the PC and home-network environments. Many,

many companies have operated in this space, including ContentGuard, Intertrust, Liquid Audio, Microsoft, Real Networks, Secure Media, and others.

While DRM technologies may provide for secure delivery of digital content to the PC and home network environment, the existing PC architecture leads to a number of vulnerabilities that may expose such content to unauthorized access and redistribution once it arrives at its destination. For example, because the PC is user programmable, it is possible to install and run circumvention utilities and non-compliant "hacked" software media players that can circumvent the technological protections or the usage permissions associated with copyrighted audiovisual content. Moreover, software-based DRM systems are more vulnerable to security breaches than are hardware-based systems as software-based DRM system must rely on tamper resistant software techniques to prevent circumvention by end-users. Even protected content may be exposed to unauthorized copying and redistribution whenever it passes over user-accessible buses or when transmitted over unprotected outputs to displays.

These vulnerabilities have led to an increased focus on trusted computing technologies, or technologies that are intended to combine hardware (such as smart cards and silicon chips) and software solutions to provide a secure trusted platform for exchanging digital content and information. Examples include an initiative by Microsoft labeled Palladium (*see* http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp), as well as efforts by smart card technology providers such as Wave Systems (*see* http://www.wave.com/technology/trustedpc_1.html) and Gemplus (see http://www.gemplus.com/).

Finally, one of the biggest sources of pirated movies on p2p networks is the big screen itself. All too often movies appear on p2p networks while they are still in the theaters because someone has simply gone into the theater with a camcorder and recorded the movie directly from the screen. In some cases these individuals use sophisticated digital recorders and plug directly into the audio sources provided for the hearing impaired – or even the theater's sound system itself – to produce a high quality camcorded version of the movie. That copy is then uploaded to a computer, digitally compressed, and redistributed to the world using p2p technology.

Recently the National Institute of Standards and Technology (NIST) announced it had awarded a $2 million grant to a company named Cinea to help fund a two-year project to develop and test prototype technology for use in distorting unauthorized recordings of digitally projected movies in a manner that is imperceptible to the human eye. More information about this company, its technology and the recent grant is available at http://www.cinea.com.

2. Limiting the Proliferation of Copies that Escape the Protected Environment

Unfortunately, no matter how good a technology is, it will always be susceptible to defeat. Thus, any meaningful framework of digital content protection must include a means of limiting the proliferation of those unauthorized copies that inevitably will escape the protected framework. This is particularly important given the fact that a single unauthorized copy of a digitized copyrighted work can populate an entire p2p network in a matter of hours.

There are a variety of technologies that now enable – and undoubtedly many more under development – tracking of infringement on p2p networks. These include, but are certainly not limited to, Ranger Online, WideVine, BayTSP, MediaForce, Cyveillance, NetPD and Media Defender. Some technologies claim to be able to identify infringing content based on unique fingerprints or content "DNA", such as BayTSP, WideVine, and Audible Magic. Some technologies offer so-called "self help" mechanisms to limit p2p infringement, such as spoofing and decoys or interdiction. Still other technologies are in use by universities, businesses, and others to control abuses of their networks by p2p users. These include, once again among others, L7 by Akonix, PacketShaper by Packeteer, Packethound by Palisade, PeerVu by Transparency Software, Employee Internet Management (EIM) by Websense, NetPure and NetEnforcer by Allot Communications, and GlobalVelocity.

Finally, existing technologies, like watermark content control information, have the potential for use in new security architectures to provide for record control, copy control, and playback control in the digital networked environment. To some extent such systems already exist. For example, a 4C CPRM licensed player is required to look for a watermark in an unencrypted disc and would refuse to play "copy never" or "copy once" content, recognizing that the unencrypted disc by definition must have been made without authorization. Similar systems might be developed for implementation across devices in the networked environment, although little progress has been made in this area, which will require cooperation and agreement by a broad range of interests.

III. Open Broad-Based Consensus Processes

The Request for Written Comments asks for information about technological protection systems developed in private voluntary industry-led entities through an open broad based consensus process. There are many such processes ongoing, in a number of forums, and MPAA is pleased to participate in several of them, including the CPTWG, DVB, MPEG, CEN-ISSS, OpenCable and others. The National Institute of Standards and Technology has undertaken to compile a "Quick Reference List of Common Terms, Organizations and Standards for Digital Rights Management" that includes a description of many of these processes, organizations and forums. A copy of the latest draft is attached. MPAA will be pleased to provide any additional information that will be of use to the PTO and the Copyright Office regarding its participation in and the work of these processes, organizations and forums.

IV. Conclusion

MPAA is pleased to have the opportunity to respond to the Request for Written Comments. While MPAA and its member companies are not generally viewed as "technology providers" per se, we are extremely active in the activities surrounding the shaping of the content protection landscape and standards setting in this area. Hopefully these comments will be of use in providing an overall context for the study to be undertaken by the PTO. MPAA will be pleased to provide whatever additional information or assistance may prove useful, including by being available to participate in the tentatively scheduled February 4 hearing.